Danville Area Community College #507
Information Security Plan
Procedures

These Procedures should be utilized in conjunction with the Information Security Plan.

Definitions

"Covered Data" means all information required to be protected under the GLB Act. The data includes information obtained from a customer and employee in the course of offering a financial product or service, or such information provided to the College from another institution. Examples of financial information relating to such products or services are bank and credit card account numbers, income and credit histories, social security numbers, student loan information, income tax information from a current or prospective student as a part of a financial aid application, and billing account financial information. Covered data consists of both paper and electronic records that are handled by the College or its affiliates.

"Service Providers" refers to all third parties who, in the ordinary course of College business, are provided access to covered data. Service providers may include business retained to transport and dispose of covered data, collection agencies, tuition payment plan companies, student loan servicers, banks, and systems support providers, for example

Procedures

(A) Physical record security safeguards.

(1) As a general rule, credit card information shouldn't be written down and should be processed in the Cashier's office. In certain, unusual circumstances, it is necessary for the Cashier's Office to write down credit card information. In this event, the information is entered into the system as soon as possible and the written credit card information is immediately shredded. Credit card information is not stored (paper or electronic). Under no circumstances should any office retain a copy of credit card information.

(2) Departments should abide by all Federal, State, Local and/or oversight agency record retention laws, policies, regulations, etc., including, but not limited to, Board Policy 4041.0 (Personnel Records), 6032.0 (Retention of College Records) and the State of Illinois Local Records Act.

(3) Offices that maintain customer information take the following security precautions:

(a) Social Security Numbers should not be written down unless required for specific processes. If they are needed, provisions should be made to safeguard and destroy them as noted by the security safeguards in these procedures.

(b) Cash receipts and cash receipt processing are conducted in an office area that has limited public access.

(c) Customer information is stored in secure areas.

(d) Retention and history files containing customer information are maintained in a secured, non-public area with limited access;

(e) Customer information that exceeds the College's retention requirements is destroyed by shredding;

(f) All staff are encouraged and reminded to sign off or lock their computers when leaving the immediate area for any length of time.

(g) Student employees working in affected offices are only provided limited access sufficient to perform their job responsibilities;

(h) All computers are turned to face College employees rather than customers or limited viewing screens are added to monitors to avoid inadvertent or unauthorized screen viewing; or any other option to limit viewing by unauthorized persons.

(i) Faculty who physically display a printed form with grades cannot display student name, student identification number, social security number or any other secure information. Alternatively, a random number should be generated and given to each student. WebAdvisor, Blackboard, or direct student communication are preferred methods.

(j) Physical records should be stored in a secure area. Only authorized employees have access to the area.

(k) Paper records should be stored in a room, cabinet, or other container that is protected when unattended.

(i) Storage areas are protected against destruction or potential damage from physical hazards or electronic backup is available to replace records.

(l) Dispose of customer information in a secure manner

(i) Customer information recorded on paper must be shredded or stored in a secure area until a shredding service picks it up.

(ii) When disposing of electronic media that contains customer information, all data must be destroyed.

(m) Maintain a close inventory of computers

(i) A close inventory of computers connected to the campus network will be constantly maintained by an automated network-based system, and will be reviewed periodically.

(ii) Maintain a system that prevents unknown computer systems from being given access to the same virtual networks as known DACC-owned systems.

(n) Unencrypted customer information should not be stored on removable media.

(B) Miscellaneous security safeguards.

(1) Human Resources will perform background or reference checks or other forms of confirmation as prudent in the hiring process for certain new employees, and implement such procedures if merited. *(See Board Policy #4012.1)*

(2) Each department that handles or maintains customer information implements those precautions it deems to be necessary and appropriate to protect customer information from destruction, loss or damage due to environmental hazards, such as fire and water damage or technical failures.

(a) The M.I.S. department has created and maintains a disaster recovery plan (the "Functional Preparedness Manual"). It is periodically reviewed and updated. The document includes sections on system hardware and software configuration, emergency contacts, information retention, normal and special procedures, and special forms used by the department. One copy is kept in the fire-resistant, locked cabinet in "off-site" storage; another copy is kept in the Director of Administrative Data Systems' office. This document would be used in the event of a disaster recovery situation as a "starting point" for personnel needing basic knowledge of our systems. The document includes many recovery procedures and can be used to build other processes in response to differing situations.

(b) Individuals with electronic created documents containing covered data will maintain a frequent schedule for creating electronic backups and updates.

(C) Network Security Safeguards.

(1) Provide for secure data transmission (with clear instructions and simple security tools) when you collect or transmit customer information.

(a) SSL (Secure Sockets Layer) is used to encrypt web-based login information and other sensitive information transmitted on the network.

(b) Data transmission to/from external vendors relies on secure transmission protocols. In most cases of data exchange between DACC and another vendor, we use software provided by the third-party vendor to supply a secure 'pipe' for transmission facilities**.**

(c) Credit Card numbers should be encrypted when transmitted.

(2) Provide for secure physical media storage.

(a) Store hard-copy documents with security –sensitive information in a locked limited-access area.

(b) Store electronic information on a secure server that is accessible only with a secure password –or has other security protections—and is kept in a physically-secure area.

(c) Maintain secure backup media and keep archived data secure by storing off-line and in a physically-secure "off-site" area with limited access. Backup procedures are in place that maintain adequate multi-generation backups for all computer data and software on the mainframe system and are rotated on a daily basis.

(3) Server and Network Hardware and Main Frame System Security

(a) DACC network equipment is stored in locked closets or cabinets to prevent physical access. Likewise, the primary campus data room, which contains several network devices and servers, and the mainframe computer room is secured with a special lock and/or an intrusion alarm system.

(4) Software Security Safeguards

(a) Ensure that only authorized employees have access to protected data.

(i) Passwords are utilized for access to e-mail, electronic data resources, shared documents, etc.

(ii) Workstations require a password to operate therefore limiting access to users' documents where feasible.

(iii) Users are to keep passwords hidden in a secure area and not share among co-workers or post in public areas.

(b) Users are blocked from installing software themselves since this might compromise the security of the workstation and the network.

(c) Access to the administrative mainframe system from off-campus sites, including home computers must establish secure "tunnels" thus encrypting the data stream. DACC off-site locations that provide network access are secured with a VPN connection.

(d) Anti-virus software should be installed and used on all workstations, servers and throughout the computer network system.

(D) Employee Management and Training

(1) Administrative staff involved in the hiring process will ensure that references are obtained prior to the conditional offer of employment.

(2) The Information Security Team in coordination with Human Resources and any appropriate individuals in affected departments, will provide and train employees who have access to covered data. Individuals will receive training on the importance of the confidentiality and disposal of customer information and protected data. They will also receive training in the proper use of computer information, passwords, procedures and protocols implemented to prevent individuals from providing confidential information to unauthorized individuals. This training would include:

(a) Locking rooms and file cabinets where paper records are kept.
(b) Avoid posting passwords near employees' computers.
(c) Encrypting sensitive customer information when it is transmitted electronically over networks or stored online.
(d) Referring calls or other requests for customer information to designated individuals who have had safeguards training.
(e) Freedom of Information Act (FOIA), or similar, requests should be directed to the FOIA Officer.

(f) Recognizing any fraudulent attempt to obtain customer information and reporting it to the Information Security Team.

(g) Learning appropriate disposal methods for protected customer information.

(3) Ask every new employee to read the Information Security Plan and Procedures to become familiar with the safeguarding procedures that they should follow in their area of employment. *(Include in new hires packet for F/T and P/T)*

(4) Instruct and regularly remind all employees of your organization's policy – and the legal requirement—to keep customer information secure and confidential. (*Communicate through Plain Brown Rapper, e-mail, opening session, etc)*

(5) Limit access to customer information to employees who have a business reason for seeing it. For example, grant access to customer information files to employees who respond to customer inquiries, but only to the extent they need it to do their job.

(E) Selection of Appropriate Service Providers.

(1) Service providers that will maintain or regularly access customer information shall be evaluated by theInformation Security Team, in conjunction with appropriate individuals from the College, prior to selection to determine their ability to safeguard customer information.

(2) Contracts with service providers that will maintain or regularly access customer information may include the following provisions:

(a) An explicit acknowledgment that the contract allows the service provider access to customer information;

(b) A specific definition or description of the customer information being provided to the service provider;

(c) A stipulation that the service provider will hold customer information in strict confidence and will only access the information for the explicit business purpose of the contract;

(d) An assurance that the service provider will protect the customer information it receives according to commercially acceptable standards and no less rigorously than it protects its own confidential information;

(e) A provision providing for the return or destruction of all customer information the service provider receives during the course of the contract upon completion or termination of the contract;

(f) An agreement that any violation of the contract's confidentiality conditions may constitute a material breach of the contract and entitle Danville Area Community College to terminate the contract without penalty;

(g) An agreement that the service provider will indemnify and hold the College harmless from any damages resulting from the contract's confidentiality conditions; and

(h) A provision ensuring that the contract's confidentiality requirements shall survive any termination agreement.

Adopted: 2-5-2005

Revised: 10-13-2017